Rafey Balabanian (SBN 315962)
rbalabanian@edelson.com
Jared Lucky (SBN 354413)
jlucky@edelson.com
EDELSON PC
150 California Street, 18th Floor
San Francisco, California 94111
Tel: 415.212.9300
Fax: 415.373.9435

Schuyler Ufkes*
sufkes@edelson.com
EDELSON PC
350 North LaSalle Street, 14th Floor
Chicago, Illinois 60654
Tel: 312.589.6370
Fax: 312.589.6378

**Pro hac vice admission to be sought*

Counsel for Plaintiff and the Putative Class

IN THE UNITED STATES DISTRICT COURT

FOR NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

ALEX WOODS, individually and on behalf of all others similarly situated,

Plaintiff,

v.

VERVE GROUP, INC., a Delaware corporation,

Defendant.

Case No.:

CLASS ACTION COMPLAINT FOR:

(1) Violation of Cal. Penal Code § 638.51;
(2) Violation of Cal. Penal Code § 502; and
(3) Violation of Cal. Penal Code § 631.

AND DEMAND FOR JURY TRIAL

Plaintiff Alex Woods ("Plaintiff" or "Woods") brings this Class Action Complaint and Demand for Jury Trial against Verve Group, Inc. ("Verve" or "Defendant") for surreptitiously tracking and selling California residents' sensitive movements and locations. Plaintiff alleges as follows upon personal knowledge as to himself and his own acts and experiences, and, as to all other matters, upon information and belief.

NATURE OF THE ACTION

1. Defendant Verve is an ad tech company and a data aggregator that surreptitiously collects and sells information about consumers from their mobile devices.

2. Verve developed and disseminated a software development kit ("SDK") that enables backdoor access to consumers' devices and opens a direct data collection pipeline to Verve and its advertising platform monetization partners. Thousands of developers have embedded Verve's SDK into their mobile apps, allowing them to siphon data from more than 2 billion consumer devices around the world.

3. The data that Verve collects from unsuspecting consumers is incredibly sensitive. Verve collects timestamped geolocation data that reveals where a consumer lives and works, and which locations they frequent. The collected location data reveals sensitive information about each consumer, such as their religious affiliation, sexual orientation, and medical conditions. This enormous volume of data enables Verve and its monetization partners to build and sell comprehensive profiles of each consumer that includes their movements and whereabouts.

4. Verve ensures that none of the data it collects from consumers' devices remains anonymous. By using its "identity graphs" process, Verve ingests and analyzes what it describes as a "treasure trove of identifiers" it obtained from mobile apps and third-party data providers to not only create a comprehensive profile on a consumer but also cross-reference and correlate various device identifiers with personal information to ascertain a consumer's identity.

5. Plaintiff and the putative Class are consumers whose sensitive data, including their location data, has been collected by Verve in violation of Cal. Penal Code § 638.51, Cal. Penal Code § 502, and Cal. Penal Code § 631. Neither Plaintiff nor any member of the putative Class has ever agreed to allow Verve to collect or sell their sensitive data and there is no mechanism to opt out of Verve's data collection practices.

PARTIES

6. Plaintiff Alex Woods is a natural person and citizen of the State of California.

7. Defendant Verve Group, Inc. is a corporation organized and existing under the laws

of Delaware with its principal place of business located at 350 5th Avenue, Suite 7700, New York, New York 10118.

JURISDICTION AND VENUE

8. This Court has jurisdiction over this action pursuant to 28 U.S.C. § 1332(d)(2) because (i) at least one member of the Class is a citizen of a different state than any Defendant, (ii) the amount in controversy exceeds $5,000,000, exclusive of interests and costs, and (iii) none of the exceptions under that subsection apply to this action.

9. This Court has personal jurisdiction over Defendant because Defendant conducts business in this District, including, on information and belief, contracting with Ifwe, Inc.—which is also headquartered in California—to embed Defendant's SDK into the Tagged app. Further, a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in the District.

10. Venue is proper pursuant to 28 U.S.C. § 1391(b) because Plaintiff resides in this District and a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in the District.

DIVISIONAL ASSIGNMENT

11. Pursuant to Civil Local Rule 3-2(c)–(d), this case should be assigned to the San Jose Division because a substantial part of the events or omission giving rise to the claim occurred within the county of Santa Clara.

COMMON FACTUAL ALLEGATIONS

Verve Surreptitiously Collects Precise Location Information from Billions of Mobile Devices

12. Verve Group is an ad tech company and a data aggregator. Their business model is to collect information from consumers, repackage and append the information, and sell access to its ill-gotten data to advertisers as well as other data brokers. Among the sensitive data Verve collects from consumers is timestamped geolocation data.

13. The secret to Verve's data pipeline is the collection of what the ad industry calls "first-party data," or data collected directly from consumers. Verve accomplishes this task by developing a SDK called "PubNative."

14. SDKs are a collection of reusable and packaged pieces of computer code that perform specific functions and processes. Software developers can integrate SDKs into their applications to save time and execute specific tasks.

15. Various developers have integrated Defendant's PubNative SDK into their mobile apps. On information and belief, over five thousand mobile apps have embedded Verve's SDK. These apps include, among others, productivity, dating, photography, and gaming apps. Verve's parent company claims that its SDK is on over 2 billion devices worldwide.

16. Verve surreptitiously collects sensitive data from consumers through its PubNative SDK. Verve collects precise and timestamped latitude and longitude geolocation coordinates from consumers' devices, mobile advertising IDs ("MAIDs"), the mobile app name, and device fingerprint data.

17. Device fingerprint data includes information about the consumer's hardware and software such as their device make and model, their device's screen resolution, current operating system version, the amount of available and used disk space on their device, and battery level, among others.

18. The problem with Verve's SDK is that consumers do not know that by interacting with an app which has embedded the PubNative SDK that their sensitive data is being surreptitiously siphoned off by an unknown third party. Consumers are never informed about Verve's SDK nor are they allowed to opt-in or opt-out of Verve's data collection practices—if they even know who or what PubNative and Verve are.

19. Indeed, when enabling location services within an app—for example a dating app or a weather app that necessarily requires the consumer to share his or her location *with the app*—the consumer grants consent *for only the mobile app* to use his or her location. At no point does Verve inform consumers that its SDK is collecting their sensitive geolocation data, nor does it prompt consumers to grant Verve permission to access or collect any data whatsoever.

20. On information and belief, a consumer would never know that any given app has the PubNative SDK third-party tracking software embedded. The entire data collection process takes place surreptitiously without the consumer's knowledge or consent.

Verve Ensures that Collected Consumer Data Does Not Remain Anonymous

21. As a preliminary matter, geolocation information is sensitive data that necessarily reveals a consumer's identity. Geolocation coordinates together with timestamp data—exactly the type of data Defendant Verve collects through its PubNative SDK—can reveal a consumer's home address, work address, and any other location they visit.

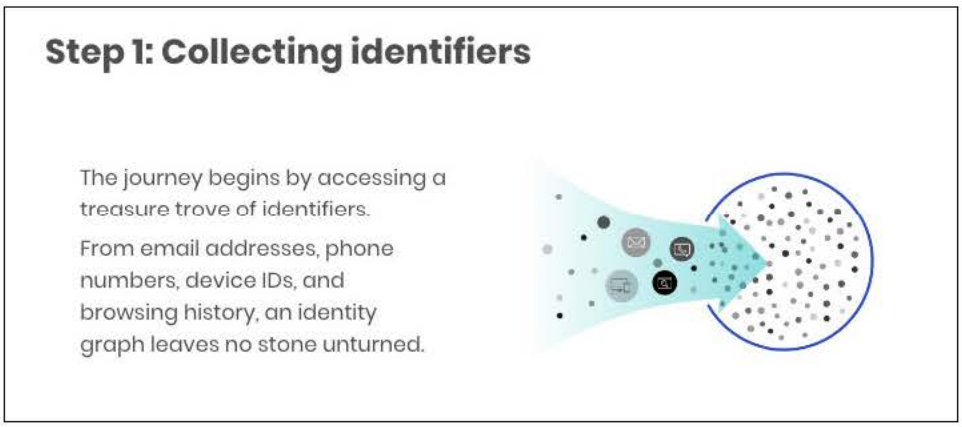
22. Indeed, researchers from MIT found that a small location data sample is sufficient to identify an individual. The researchers analyzed timestamped location data for 1.5 million individuals over 15 months and found that only four timestamped locations are sufficient to identify 95% of individuals. Given 11 data points, the researchers could identify all individuals in the study. The reason for the findings is obvious: individuals have unique movement patterns, and it is not likely that someone else will be in the same locations at four different times of the day.

23. The researchers commented that an individual may be identified with less than four data points simply by exploiting irregularities in an individual's behavior.

24. By collecting timestamped geolocation data, MAIDs, and device fingerprint data, Verve can connect an ostensibly "anonymous" ID (such as a MAID) to an individual and then collect data on their interests and activities across the internet.

25. Verve touts that it uses a technology it calls "identity graphs" to identify consumers across various platforms and screens. Verve states that its identity graphs technology is the reason behind "emails that address you by your first name to ads that eerily know your shopping preferences." It explains, "an identity graph is like a digital Rolodex, but incredibly smarter. It is an online database that meticulously stores identifiers tied to individual customers and prospects, providing businesses with a 360-degree view of their audiences across diverse channels."

26. Verve explains how its identity graphs technology works. First, Verve "begins by accessing a treasure trove of identifiers. From email addresses, phone numbers, device IDs, and browsing history, an identity graph leaves no stone unturned." *See* Figure 1.

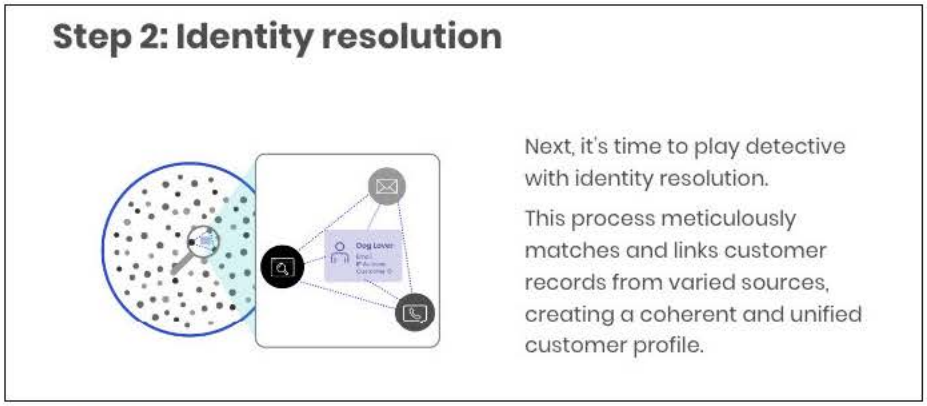


(Figure 1 showing Verve's collection of "a treasure trove of identifiers.")

27. A discussed above, Verve collects various identifiers such as MAIDs, timestamped geolocation information, device fingerprint information, as well as information about their app usage and online activities. Furthermore, Verve purports to obtain even more data from third-party data providers such as Comcast, Oracle, and ID5, among others. *See* Figure 2. ID5, for example, is a company that "provides identification services" and promises to provide its customers (like Verve) "comprehensive identification capabilities."

(Figure 2)

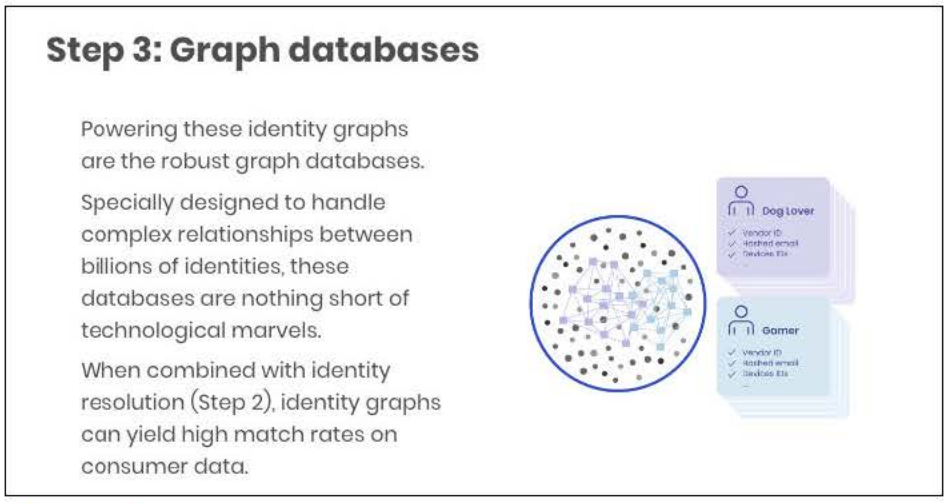
28. The second step of Verve's identity graph is its "identity resolution" step that "meticulously matches and links customer records from varied sources, creating a coherent and unified customer profile." *See* Figure 3.



(Figure 3)

29. Verve plays "detective" by matching various identifiers it has obtained directly from a consumer with data it bought from third-party providers to create a profile on the consumer. For example, Verve can cross-reference a record of a consumer having visited a specific location with a record of a consumer having downloaded a certain app because both records share a common device ID.

30. The third step of Verve's identity graph is to store the various links and relationships it has matched into a database. This database is "specially designed to handle complex relationships between billions of identities" and "can yield high match rates on consumer data." *See* Figure 4.



(Figure 4)

31. Most importantly, Verve collects and updates its identity graphs database in real time. That means should a consumer change his or her MAID, for example, Verve will be able to continue to identify and track the consumer. Similarly, should a consumer download a new app or

visit a new location, Verve's identity graphs will immediately know and update its database. Verve states, "identity graphs ensure businesses have the freshest view of their customers by updating in real-time."

Verve's Data Collection Reveals Sensitive Information About Consumers

32. Verve's practice is far from inconsequential. Its surreptitious and routine collection of precise geolocation data reveals locations associated with medical care, reproductive health, religious worship, mental health, and temporary shelters, such as shelters for the homeless, domestic violence survivors, or other at-risk populations, and addiction recovery centers. As such, Verve's data collection may reveal, for instance, a consumer's religious affiliation, sexual orientation, medical condition, and even whether the consumer is part of an at-risk population.

33. Verve has fingerprinted consumers and has correlated a vast amount of personal information about them not only from its surreptitious SDK but also from third-party data brokers—entirely without consumers' knowledge and consent. Verve has created profiles on consumers and its graph database holds information about consumers' interests, the locations they have visited, and the names of apps they have downloaded.

34. To make matters worse, Verve monetizes and sells its collected data—specifically the timestamped geolocation data, MAIDS, and device fingerprint data—to advertising platforms and advertisers.

35. Verve has partnered with various advertising demand side platforms (or "DSPs"). DSPs are where advertisers and agencies go to purchase digital advertisement inventory. According to Verve, it has partnered with over 30 various DSPs which it considers its "monetization partners.[1]" Most concerning is that Verve purports to exchange "Precise Geographic Location Data" with its DSPs and, in turn, any advertiser who seeks to purchase advertisements and/or consumer data.

[1] *Monetization Partners*, PubNative, https://pubnative.net/monetization-partners/ (last visited Aug. 5, 2024).

36. Verve's collection of sensitive geolocation data has enabled a host of third parties with access to such data to track consumers down to sensitive locations and track their every movement. Verve has not published a full list of third-party data purchasers, but the types of third parties benefiting from Verve's data may include advertising agencies, Fortune 500 companies, advertising platforms, and even government agencies. Verve's parent company claims that brands like McDonalds, Bank of America, Pepsico, Uber, and TikTok, among others, leverage Verve's advertising (and tracking) capabilities.

37. A government contractor named Mike Yeagley recently explained how the Pentagon finds its targets. Yeagley leveraged SDKs embedded in various mobile apps that transmit geolocation data to advertisement networks to obtain near real-time coordinates on his targets. Furthermore, Yeagley created geofences around government buildings to identify which devices—and subsequently which individuals—visited what building, where these individuals went afterwards, and with whom they associated.

38. Yeagley's use of the data shows not only how the United States might deploy this technology to track consumers, but also how this easily accessible location data could allow America's adversaries to purchase the same type of information and use it to track American residents.

39. The Defense Intelligence Agency ("DIA") and the National Security Agency ("NSA") have also previously purchased geolocation data surreptitiously collected from American consumers' devices. Similarly, the Department of Homeland Security ("DHS") has purchased more than 200 licenses since 2019 from vendors who broker location data from consumer devices.

40. Ron Wyden, a senator from Oregon, in a letter to the FTC, has harshly criticized the practice of government agencies purchasing geolocation data on American consumers and blamed advertisers and developers for failing to disclose such data collection practices: "App developers and advertising companies did not meaningfully disclose to users their sale and sharing of personal data with data brokers nor seek to obtain informed consent."

41. Ultimately, the PubNative SDK has allowed Verve to secretly create a detailed log of Plaintiff's and the putative Class's precise movement patterns, along with a dossier of their likes and interests, all without their consent or permission.

FACTS SPECIFIC TO PLAINTIFF

42. Plaintiff Woods downloaded and used the "Tagged" dating app on his Android device within the last year.

43. To use the "Tagged" mobile app, Plaintiff enabled location services for the sole purpose of sharing his location with "Tagged." The developers of the "Tagged" mobile app have embedded the PubNative SDK into their mobile app, allowing Defendant to collect Plaintiff's timestamped geolocation information, device IDs, device fingerprint data, and information about which app(s) he uses on his mobile device.

44. Plaintiff did not (and could not) grant Defendant permission to collect any information—especially not precise geolocation information—from his device whatsoever.

CLASS ACTION ALLEGATIONS

45. **Class Definition**: Plaintiff Alex Woods brings this proposed class action pursuant to Federal Rule of Civil Procedure 23(b)(2) and Rule 23(b)(3) on behalf of himself and a Class of others similarly situated, defined as follows:

> All California residents who downloaded and used an app on their mobile device (1) with the PubNative SDK embedded into the app and (2) that did not publicly disclose "Verve" or "PubNative" in any of the app's notices or disclosures.

Excluded from the Class are: (1) any Judge or Magistrate presiding over this action and members of their families; (2) Defendant, Defendant's subsidiaries, parents, successors, predecessors, and any entity in which Defendant or its parents have a controlling interest and its officers and directors; (3) persons who properly execute and file a timely request for exclusion from the Class; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiff's counsel and Defendant's counsel; and (6) the legal representatives, successors, and assigns of any such excluded persons.

46. **Numerosity**: The exact number of Class members is unknown and not available to Plaintiff at this time, but it is clear that individual joinder is impracticable. On information and belief, Defendant has surreptitiously collected timestamped geolocation information from millions of consumers who fall into the definition of the Class. Class members can be identified through Defendant's records.

47. **Commonality and Predominance**: There are many questions of law and fact common to the claims of Plaintiff and the putative Class, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class include, but are not necessarily limited to the following:

(a) Whether Defendant used a pen register;

(b) Whether Defendant obtained consent from Plaintiff and the Class or otherwise obtained a warrant to install and use a pen register;

(c) Whether Defendant accessed Plaintiff's and the Class's computer systems;

(d) Whether Defendant made an unauthorized connection with Plaintiff's and the Class's mobile devices; and

(e) Whether Defendant used or attempted to use any information obtained from Plaintiff's and the Class's mobile devices.

48. **Typicality**: Plaintiff's claims are typical of the claims of the Class members in that Plaintiff, like all Class members, has been injured by Defendant's misconduct at issue.

49. **Adequate Representation**: Plaintiff will fairly and adequately represent and protect the interests of the Class and has retained counsel competent and experienced in complex litigation and class actions. Plaintiff's claims are representative of the claims of the other members of the Class. That is, Plaintiff and the Class members sustained damages as a result of Defendant's conduct. Plaintiff also has no interests antagonistic to those of the Class, and Defendant has no defenses unique to Plaintiff. Plaintiff and his counsel are committed to vigorously prosecuting this action on behalf of the members of the Class and have the financial resources to do so. Neither Plaintiff nor his counsel has any interest adverse to the Class.

50. **Superiority**: Class proceedings are superior to all other available methods for the fair and efficient adjudication of this controversy, as joinder of all members of the Class is impracticable. Individual litigation would not be preferable to a class action because individual litigation would increase the delay and expense to all parties due to the complex legal and factual controversies presented in this Complaint. By contrast, a class action presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court. Economies of time, effort, and expense will be fostered, and uniformity of decisions will be ensured.

51. Plaintiff reserves the right to revise the foregoing "Class Allegations" and "Class Definition" based on facts learned through additional investigation and in discovery.

FIRST CAUSE OF ACTION
Violation of California Invasion of Privacy Act
Cal. Penal Code § 638.51
(On behalf of Plaintiff and the Class)

52. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

53. California law prohibits the installation of a pen register without first obtaining a court order. Cal. Penal Code § 638.51.

54. The statute defines a "pen register" as "a device or process that records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, but not the contents of a communication." Cal. Penal Code § 638.50(b).

55. Defendant's PubNative SDK is a "pen register" because it is a device or process that records addressing or signaling information—in this instance, Plaintiff's and the Class members' location and personal information—from electronic communications transmitted by their devices. Furthermore, Defendant's SDK is a device or process that identifies consumers, gathers data, and correlates data through sophisticated device fingerprinting and its "identity graph" functionality.

56. Defendant was not authorized by any court order to use a pen register to track Plaintiff's and Class members' location and personal information, nor did it obtain consent from

Plaintiff and the Class to operate such a device.

57. Plaintiff and the Class seek injunctive relief and statutory damages in the amount of $5,000 per violation pursuant to Cal. Penal Code § 637.2.

SECOND CAUSE OF ACTION
Violation of the California Comprehensive Computer Data Access and Fraud Act
Cal. Penal Code § 502
(On behalf of Plaintiff and the Class)

58. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

59. The California Legislature enacted the Comprehensive Computer Data Access and Fraud Act ("CDAFA") to "expand the degree of protection afforded to individuals . . . from tampering, interference, damage, and unauthorized access to lawfully created computer data and computer systems." Cal. Penal Code § 502(a). In enacting the statute, the Legislature emphasized the need to protect individual privacy: "[The] Legislature further finds and declares that protection of the integrity of all types and forms of lawfully created computers, computer systems, and computer data is vital to the protection of the privacy of individuals[.]" *Id.*

60. Plaintiff's and the Class members' mobile devices are "computers" or "computer systems" within the meaning of § 502(b) because they are devices capable of being used in conjunction with external files and perform functions such as logic, arithmetic, data storage and retrieval, and communication.

61. Defendant violated the following sections of CDAFA § 502(c):

a. "Knowingly accesses and without permission . . . uses any data, computer, computer system, or computer network in order to . . . wrongfully control or obtain money, property, or data." *Id.* § 502(c)(1).

b. "Knowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network." *Id.* § 502(c)(2).

c. "Knowingly and without permission accesses or causes to be accessed any computer, computer system, or computer network." *Id.* § 502(c)(7).

62. Defendant "accessed" Plaintiff's and the Class members' computers and/or computer

systems because it gained entry to and/or caused output from their mobile devices to obtain geolocation information and personal information.

63. Defendant was unjustly enriched with the data it obtained from Plaintiff and the Class.

64. Plaintiff and the Class now seek compensatory damages, injunctive relief, disgorgement of profits, other equitable relief, punitive damages, and attorneys' fees pursuant to § 502(e)(1)–(2).

THIRD CAUSE OF ACTION
Violation of California Wiretap Act
Cal. Penal Code § 631
(On behalf of Plaintiff and the Class)

65. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

66. The California Wiretap Act, Cal. Penal Code § 631, prohibits:

> Any person [from using] any machine, instrument, or contrivance, or in any other manner . . . [from making] any unauthorized connection, whether physically, electrically, acoustically, inductively, or otherwise, with any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system, or who willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state; or who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained, or who aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section[.]

67. Defendant's SDK tracked Plaintiff's and Class members' specific input events and choices on their mobile devices such as their movements and affirmative actions such as installing a mobile app on their device and therefore constitute communications within the scope of the California Wiretap Act.

68. Defendant's PubNative SDK made an unauthorized connection with Plaintiff's and Class members' devices and obtained their sensitive information including their movements, geolocation information, mobile device IDs, device fingerprint data, and information about the mobile app(s) they downloaded.

69. Furthermore, Defendant attempted to and did sell or otherwise share the data it wrongfully obtained from Plaintiff and the Class to third parties including advertising DSPs and other advertisers.

70. Defendant never obtained any consent whatsoever from Plaintiff and the Class.

71. Plaintiff and the Class seek an injunction and damages in the amount of $5,000 per violation pursuant to Cal. Penal Code § 637.2.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff Alex Woods individually and on behalf of the Class, prays for the following relief:

(a) An order certifying the Class as defined above, appointing Alex Woods as the representative of the Class, and appointing his counsel as Class Counsel;

(b) An order declaring that Defendant's actions, as set out above, violate the California Invasion of Privacy Act, Cal. Penal Code § 638.51; violate the California Comprehensive Computer Data Access and Fraud Act, Cal Penal Code § 502; and violate the California Wiretap Act, Cal. Penal Code § 631.

(c) An injunction requiring Defendant to cease all unlawful activities;

(d) An award of liquidated damages, disgorgement of profits, punitive damages, costs, and attorneys' fees;

(e) Such other and further relief that the Court deems reasonable and just.

JURY DEMAND

Plaintiff requests a trial by jury of all claims that can be so tried.

Respectfully submitted,

ALEX WOODS, individually and on behalf of all others similarly situated,

Dated: August 8, 2024

By: */s/ Rafey Balabanian*
One of Plaintiff's Attorneys

Rafey Balabanian (SBN 315962)
rbalabanian@edelson.com

Jared Lucky (SBN 354413)
jlucky@edelson.com
EDELSON PC
150 California Street, 18th Floor
San Francisco, California 94111
Tel: 415.212.9300
Fax: 415.373.9435

Schuyler Ufkes*
sufkes@edelson.com
EDELSON PC
350 North LaSalle Street, 14th Floor
Chicago, Illinois 60654
Tel: 312.589.6370
Fax: 312.589.6378

**Pro hac vice admission to be sought*

Counsel for Plaintiff and the Putative Class